

# **HONE: Correlating Host activities to Network communications to produce insight**

**What if you could  
collect and analyze  
only the most  
important cyber  
security data?**

**GLENN A. FINK, PH.D.**  
Senior Scientist, Secure Cyber Systems

**SEAN STORY, PMP**  
Project Manager, Software Engineering & Architectures



# What is the problem?

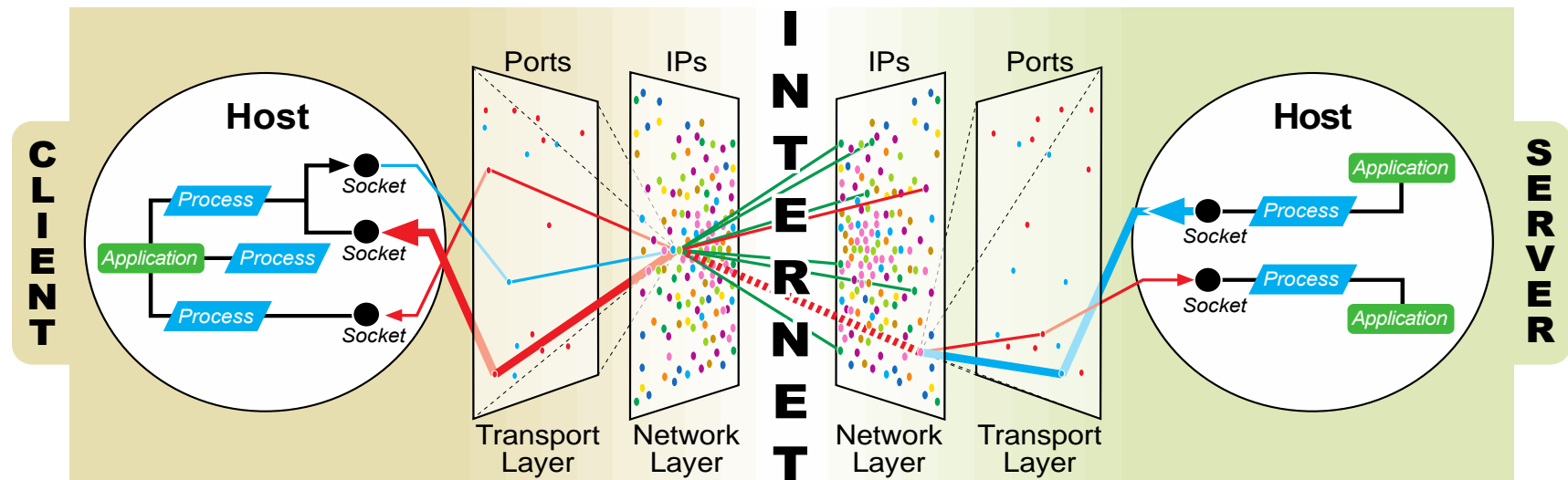
- ▶ We collect too much extraneous cyber data and then put in too much work to process it all



- ▶ Why? The design of Internet protocols makes correlation and isolating root causes of break-ins difficult

# How will we fix the problem?

- ▶ We *correlate* communications and processing activities in the kernel of the operating system
- ▶ This lets us find out what programs are responsible for malicious network activity



- ▶ Requires a kernel module on each monitored machine



# What are the benefits?

Fewer analyst hours are needed to correlate cyber data → savings



Analysts can characterize communications with 100% accuracy

Hone provides a key to understand the computer from the network



Hone keeps a persistent file of correlated machine and network activities

# What alternatives are there?

- ▶ TCPView, NetStat, and other host-based tools:
  - Can see the connections but not the actual activity
  - Use a polling approach that misses short events
- ▶ Deep-packet inspection or Dynamic Analysis
  - Expensive and potentially inaccurate
- ▶ Connection-filtering host-based firewalls
  - Only operate on the connection level, not per packet
  - Once you grant blanket permission to an application, you have no further control
- ▶ Multi-host-based security and analysis
  - Requires elaborate infrastructure

# Hone Demonstration

linux.pcapng [Wireshark 1.7.0-HONE-TEST-x64-1 (SVN Rev 37663 from /trunk)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
23	4449.28363			Process	28	FORK :: Process ID: 2737
24	4450.04382			Process	70	BEGIN :: Process ID: 2737   Path: /bin/unamept/firefox/run-mozilla.sh
25	4451.06393			Process	28	END :: Process ID: 2737
26	4452.86855			Process	89	BEGIN :: Process ID: 2731   Path: /opt/firefox/firefox-bin-mozilla.sh
27	10001.6585			Connection	12	BEGIN :: Process ID: 1220   Connection ID: 2083439552
28	10001.7745			Connection	12	END :: Process ID: 1220   Connection ID: 2083439552
29	11103.0987			Connection	12	BEGIN :: Process ID: 2731   Connection ID: 2075779200
30	11103.1490			Connection	12	END :: Process ID: 2731   Connection ID: 2075779200
31	11106.9221			Connection	12	BEGIN :: Process ID: 2731   Connection ID: 1661328128
32	-3482.8649	10.0.2.15	130.20.248.22	DNS	71	Standard query 0x3437[Packet size limited during capture]
33	-3482.8648	10.0.2.15	130.20.248.22	DNS	71	Standard query 0x95b0[Packet size limited during capture]
34	-3482.6481	130.20.248.22	10.0.2.15	DNS	133	Standard query response 0x95b0[Packet size limited during capture]
35	-3482.5050	130.20.248.22	10.0.2.15	DNS	87	Standard query response 0x3437 A[Packet size limited during capture]
36	11467.2026			Connection	12	END :: Process ID: 2731   Connection ID: 1661328128
37	11467.5992			Connection	12	BEGIN :: Process ID: 2731   Connection ID: 2056703360
38	-3482.5039	10.0.2.15	109.203.97.80	TCP	68	53799 > http [SYN] Seq=0 win=14600 Len=0[Packet size limited during capture]
39	-3482.5025	109.203.97.80	10.0.2.15	TCP	52	http > 53799 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0[Packet size limited during capture]
40	-3482.5025	10.0.2.15	109.203.97.80	TCP	48	53799 > http [ACK] Seq=1 Ack=1 win=14600[Packet size limited during capture]
41	-3482.5019	10.0.2.15	109.203.97.80	HTTP	729	GET /planet/?media=rss HTTP/1.1 [Packet size limited during capture]
42	-3482.5017	109.203.97.80	10.0.2.15	TCP	48	http > 53799 [ACK] Seq=1 Ack=682 win=65535[Packet size limited during capture]
43	11835.8205			Connection	12	BEGIN :: Process ID: 2731   Connection ID: 1661327296
44	-3482.1361	10.0.2.15	130.20.248.22	DNS	77	Standard query 0x67f9[Packet size limited during capture]
45	-3482.1360	10.0.2.15	130.20.248.22	DNS	77	Standard query 0x5561[Packet size limited during capture]
46	-3482.1344	130.20.248.22	10.0.2.15	DNS	141	Standard query response 0x67f9 A 69.195.141.179 A 82.103.140.40 A 82.103.140.42 A[Packet size limited during capture]
47	-3482.1327	130.20.248.22	10.0.2.15	DNS	139	Standard query response 0x5561[Packet size limited during capture]
48	11839.5570			Connection	12	END :: Process ID: 2731   Connection ID: 1661327296
49	11839.7940			Connection	12	BEGIN :: Process ID: 2731   Connection ID: 1661327296
50	11839.8574			Connection	12	END :: Process ID: 2731   Connection ID: 1661327296

Frame 26: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)

Hone Process Event Block

Process ID: 2731

Event: 0x00000000

Parent Process ID: 1

User ID: 1000

Group ID: 1000

Path: /opt/firefox/firefox-bin

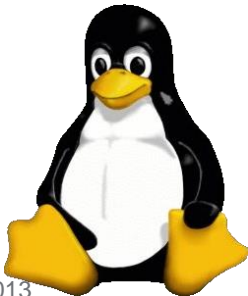
Argv: /opt/firefox/firefox-bin

0000 ab 0a 00 00 00 00 00 01 00 00 00 e8 03 00 00 .....  
0010 e8 03 00 00 19 00 00 00 19 00 00 00 2f 6f 70 74 .....  
0020 2f 66 69 72 65 66 6f 78 2f 66 69 72 65 66 6f 78 .....  
0030 2d 62 69 6e 00 2f 6f 70 74 2f 66 69 72 65 66 6f .....  
0040 78 2f 66 69 72 65 66 6f 78 2d 62 69 6e 00 00 00 .....  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

File: "D:\Applications\Hone\Workspace\linu... Packets: 8887 Displayed: 8887 Marked: 0 Load time: 0:00.510 Profile: Default

# Conclusion

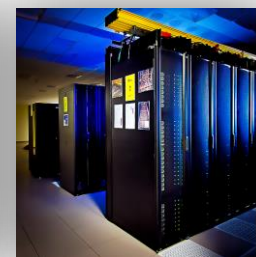
- ▶ All Internet devices use common protocols, so Hone's simple correlation will enable a revolution in defense
- ▶ Hone provides the precision to control communications at the packet level
- ▶ Hone gives trustworthy process attribution
- ▶ We are seeking partners to:
  - Sponsor follow-on work
  - Test deploy operational prototypes
  - License for use in new and existing products



August 15, 2013



# Correlating machine and network activities to produce insight



**Glenn Fink, PhD**  
Cyber Security Scientist  
[Glenn.Fink@pnnl.gov](mailto:Glenn.Fink@pnnl.gov)  
(509) 375-3994



**Sean Story, PMP**  
Project Manager  
[story@pnnl.gov](mailto:story@pnnl.gov)  
(509) 375-3612

Pacific Northwest National Laboratory  
Richland, Washington